Course Outline

MOC 40554 A Microsoft Security Workshop: Implementing Windows 10 Security Features

Course Summary

Objectives

After taking this course, students will be able to:

- Understanding the current nature of the security threat landscape
- Explain the built-in security defenses Windows 10
- Windows 10 mitigations that you can configure
- Learn the Windows 10 mitigations that require no configuration
- Describe some of the external tools that enhance endpoint security

Topics

- How Windows 10 uses modern hardware features for security
- Windows 10 software security features
- The latest Windows 10 Security-related Features

Audience

This course is intended for IT Professionals that require a deeper understanding of Windows Security and to increase their knowledge level through a predominately hands-on experience with Microsoft threat detection tools for hybrid and cloud-based workloads.

Prerequisites

In addition to their professional experience, students who take this training should already have the following technical knowledge:

The current cybersecurity ecosystem

- Experience with Windows Client and Server administration, maintenance, and troubleshooting.
- Basic experience and understanding of Windows networking technologies, to include Windows Firewall network setting, DNS, DHCP, WiFi, and cloud services concepts.
- Basic experience and understanding of Active Directory, including functions of a domain controller, sign on services, and an understanding of group policy.
- Knowledge of and relevant experience in systems administration, using Windows 10.

Learners who take this training can meet the prerequisites by obtaining equivalent knowledge and skills through practical experience as a Security Administrator, System Administrator, or a Network Administrator.

Duration

One day

Course Outline

MOC 40554 A Microsoft Security Workshop: Implementing Windows 10 Security Features

Course Outline

I. How Windows 10 uses modern hardware features for security

Today's security threat landscape is dominated by aggressive and tenacious threats. Originally, malicious attackers mostly focused on gaining community recognition through their exploits. Since then, attackers' motives have shifted toward financial gain. Modern attacks increasingly focus on large-scale intellectual property theft, targeted system degradation that can result in financial loss, and even cyberterrorism that threatens the security of individuals, businesses, and national or regional interests all over the world. Attackers are typically highly trained individuals and security experts, some of whom are in the employ of nation states that have large budgets and vast human resources. Threats like these require a different approach to cybersecurity. In this module we look at the hardware security features in the latest Windows 10 releases to help mitigate these threats.

A. Secure Boot and Unified Extensible Firmware Interface (UEFI)-based protection
B. Additional Hardware Security

II. Windows 10 software security features

Windows 10 includes a number of security features that protects your device, operating system, applications, and data. These features deliver comprehensive, built-in, and ongoing protection against cyber threats. In this module, you will learn about the most important of these features, including Windows Defender Firewall, Virtual Secure Mode, Credential Guard, Remote Credential Guard, and Device Guard, BitLocker and AppLocker, Windows Defender Antivirus, Windows Defender SmartScreen, and Windows 10 telemetry.

A. Core built-in Windows 10 security features
B. Additional built-in software security features

III. The latest Windows 10 Security-related Features

As described in the first module of this course, contemporary security threat landscape is one of aggressive and tenacious threats. In recognition of this landscape, Microsoft continues to strengthen the security posture of Windows 10 by developing new and enhance existing security features intended to make it difficult and costly to find and exploit software vulnerabilities. These features are designed to:> Eliminate entire classes of vulnerabilities> Break exploitation techniques> Contain the damage and prevent persistence> Limit the window of opportunity to exploit This module provides an overview of some of the software and firmware threats faced in the current security landscape, and the mitigations that the latest versions of Windows 10 offer in response to these threats.

A. An overview of the latest Windows 10 security-related features
B. Windows 10 Ransomware Case Study

Lab : Implementing Windows Defender Firewall with Advanced Security on Domain-joined Windows 10 Clients

- Implement end-to-end IPsec connectivity between a Windows 10 domain-joined client and a Windows Serv

Lab : Implementing BitLocker on Domain-joined Windows 10 Clients

- Encrypt non-operating system volumes by using BitLocker
- Recovering access to BitLocker-encrypted volumes

Lab : Implementing AppLocker on Domain-joined Windows 10 Clients

- Implement AppLocker on a domain-joined Windows 10 client

Lab : Implementing Windows Defender Device Guard Code Integrity on Domain-joined Windows 10 Clients

- Implement Windows Defender Device Guard Code Integrity on a domain-joined Windows 10 client

Lab : Implementing Windows Defender Remote Credential Guard and Remote Admin mode on Domain-joined Windows

- Implement Remote Desktop session protection with Remote Credential Guard
- Implement Remote Desktop session protection with Restricted Admin Mode